On the dual binary codes of the triangular graphs

B.G. Rodrigues

School of Mathematical Sciences, University of KwaZulu-Natal, Durban 4041, South Africa

Received 14 March 2005; accepted 15 July 2005
Available online 22 August 2005
Dedicated to Jamshid Moori on the occasion of his 60th birthday.

Abstract

The stabilizers of the minimum-weight codewords of dual binary codes obtained from the strongly regular graphs $T(n)$ defined by the primitive rank-3 action of the alternating groups $A_n$ where $n \geq 5$, on $\Omega^{(2)}$, the set of duads of $\Omega = \{1, 2, \ldots, n\}$, are examined.

© 2005 Elsevier Ltd. All rights reserved.

1. Introduction

The simple alternating group $A_n$, where $n \geq 5$, acts as a primitive rank-3 group of degree $\binom{n}{2}$ on the 2-subsets, $\Omega^{(2)}$, where $\Omega = \{1, 2, \ldots, n\}$. The orbits of the stabilizer in $A_n$ of a 2-subset $P = \{a, b\}$ consist of $\{P\}$, one of length $2(n-2)$ and the other of length $\binom{n-2}{2}$. We take as points the 2-subsets of $\Omega$ and for each $P \in \Omega^{(2)}$ we define a block $\overline{P}$ to be $\{Q \in \Omega^{(2)} \mid P \cap Q \neq \emptyset, Q \neq P\}$, i.e. the members of the orbit of length $2(n-2)$. The 2-subsets $P$ and blocks $\overline{P}$ form a symmetric 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design whose binary code we will be examining.

An alternative way to approach the designs, graphs and codes that we will be looking at is through the span of the adjacency matrices of the triangular graphs. For any $n$ the triangular graph $T(n)$ is defined to be the line graph of the complete graph $K_n$. It is a strongly regular graph on $v = \binom{n}{2}$ vertices, i.e. on the pairs of letters $\{i, j\}$ where
The binary codes formed from the span of adjacency matrices of triangular graphs have been examined by Tonchev [13, p. 171] and Haemers et al. [6, Theorem 4.1] and recently by Key et al. [9]. See also [3,4,1,2,12]. In particular the weight enumerators of these codes are easily determined.

The code of the 1-\((v,n,\lambda)_3\) design obtained by taking the rows of the incidence matrix as the incidence vectors of the blocks is also the code formed by the span of the adjacency matrix of the triangular graph \(T(n)\); the automorphism group of this design will contain the automorphism group of the graph, the latter of which is easily seen to be \(S_n\). Similarly, the automorphism group of the code will contain \(S_n\). However for \(n = 6\) the group of the design and code is larger than the group of the graph \((S_6)\). When \(n = 6\), the automorphism group of both design and code is the alternating group \(A_8 \cong PGL_4(2)\).

This paper has emerged as a result of [9], where permutation decoding sets were found for the binary codes from the triangular graphs. In [11], we determined the stabilizers of the minimum-weight codewords of the binary code \(C\) of the triangular graph \(T(n)\). Here, following the ideas of [11], we study the stabilizers of the minimum-weight codewords for the dual binary codes of the triangular graphs. We consider \(w\) to be a codeword of minimum weight in the dual binary code \(\perp C\) of \(C\), for any \(n \geq 5\), and determine the stabilizers \(\text{Aut}(\perp C)_w\) of \(w\) in \(\text{Aut}(\perp C)\). We show that \(\text{Aut}(\perp C)_w\) are maximal subgroups of \(\text{Aut}(\perp C)\).

In Section 2 we give the necessary definitions and background. In Section 3 we describe the nature of the minimum-weight codewords in \(\perp C\) for \(n \geq 5\), as given in [9, Lemma 3.2].

Since the alternating group \(A_n\) acts as an automorphism group of \(\perp C\), in Section 4 we determine the stabilizers \((A_n)_w\) of a codeword \(w\) of minimum weight in \(\perp C\) and show that \((A_n)_w \cong (A_{n-3} \times 3):2\), for \(n \geq 7\). In all cases, we show that \((A_n)_w\) are maximal subgroups of \(A_n\). If \(n = 5\) we have that \((A_5)_w \cong S_3\), a maximal subgroup of \(A_5\), and if \(n = 6\) we have that \((A_6)_w \cong S_4\), which is maximal in \(A_6\) or \((A_6)_w \cong (Z_3 \times Z_3):Z_2\) which is not a maximal subgroup of \(A_6\).

Furthermore, since the automorphism group of \(\perp C\) is \(S_n\), for all \(n \geq 5\) except when \(n = 6\) by extending the results of \(A_n\) to \(S_n\) we show that \((S_n)_w \cong S_{n-3} \times S_3\), for \(n \geq 5\). In all cases we have that \((S_n)_w\) are maximal subgroups of \(S_n\). If \(n = 6\) we have that \(\text{Aut}(\perp C) = A_8\) and we show that \((A_8)_w \cong 2^4:(S_3 \times S_3)\), a maximal subgroup of \(A_8\).

2. Background and terminology

Our notation will be standard, and it is as in [1] and ATLAS [5]. For the structure of groups and their maximal subgroups we follow the ATLAS notation. The groups \(G/H\), \(G : H\), and \(G/H\) denote a general extension, a split extension and a non-split extension respectively. For a prime \(p\), the symbol \(p^n\) denotes an elementary abelian group of order \(p^n\) and exponent \(p\) or \(p^2\) respectively.

An incidence structure \(D = (P, B, \mathcal{I})\), with point set \(P\), block set \(B\) and incidence \(\mathcal{I}\), is a \(t-(v,k,\lambda)\) design if \(|P| = v\), every block \(B \in B\) is incident with precisely \(k\) points, and every \(t\) distinct points are together incident with precisely \(\lambda\) blocks. The design is symmetric if it has the same number of points and blocks.
The code $C_F$ of the design $\mathcal{D}$ over the finite field $F$ is the space spanned by the incidence vectors of the blocks over $F$. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^\mathcal{Q}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^\mathcal{P}$, the full vector space of functions from $\mathcal{P}$ to $F$.

All our codes will be linear codes, i.e. subspaces of the ambient vector space. If a code $C$ over a field of order $q$ is of length $n$, dimension $k$, and minimum weight $d$, then we write $[n, k, d]_q$ to show this information. A generator matrix matrix for the code is a $k \times n$ matrix made up of a basis for $C$. The dual or orthogonal code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{ v \in F^n \mid (v, c) = 0 \text{ for all } c \in C \}$. A check (or parity-check) matrix for $C$ is a generator matrix $H$ for $C^\perp$; the syndrome of a vector $y \in F^n$ is $Hy^T$. A code $C$ is self-orthogonal if $C \subseteq C^\perp$ and is self-dual if $C = C^\perp$. If $c$ is a codeword then the support of $c$ is the set of non-zero coordinate positions of $c$. A constant vector is one for which all the coordinate entries are either 0 or 1. The all-one vector will be denoted by $j$, and is the constant vector of weight the length of the code. Two linear codes of the same length and over the same field are isomorphic if they can be obtained from one another by permuting the coordinate positions. Any code is isomorphic to a code with generator matrix in so-called standard form, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first $k$ coordinates are the information symbols and the last $n-k$ coordinates are the check symbols. An automorphism of a code $C$ is an isomorphism from $C$ to $C$. The automorphism group will be denoted by Aut($C$). Any automorphism clearly preserves each weight class of $C$.

Terminology for graphs is standard: the graphs, $\Gamma = (V, E)$ with vertex set $V$ and edge set $E$, are undirected and the valency of a vertex is the number of edges containing the vertex. A graph is regular if all the vertices have the same valency; a regular graph is strongly regular of type $(n, k, \lambda, \mu)$ if it has $n$ vertices, valency $k$, and if any two adjacent vertices are together adjacent to $\lambda$ vertices, while any two non-adjacent vertices are together adjacent to $\mu$ vertices. The line graph of a graph $\Gamma = (V, E)$ is the graph $\Gamma' = (E, V')$ where $e$ and $f$ are adjacent in $\Gamma'$ if $e$ and $f$ share a vertex in $\Gamma$. The complete graph $K_n$ on $n$ vertices has for $E$ the set of all 2-subsets of $V$. The line graph of $K_n$ is the triangular graph $T(n)$, and it is strongly regular of type $\left(\binom{n}{2}, 2(n - 2), n - 2, 4\right)$. These graphs are unique for $n \neq 8$ and for $n = 8$ there are exactly three other graphs with the same parameters, the so-called Chang graphs: see [4,6].

The codes are the binary span of the adjacency matrix of the graph. The $p$-rank of these has been studied by various authors; see [3,6] for collected results.

The designs and codes in this paper come from the following standard construction, described in [7, Proposition 1] and in [8]:

**Result 2.1.** Let $G$ be a finite primitive permutation group acting on the set $\Omega$ of size $n$. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $G_\alpha$ of $\alpha$. If

$$\mathcal{B} = \{\Delta^g : g \in G\}$$

and, given $\delta \in \Delta$,

$$\mathcal{E} = \{\{\alpha, \delta\}^g : g \in G\},$$

The codes are the binary span of the adjacency matrix of the graph. The $p$-rank of these has been studied by various authors; see [3,6] for collected results.

The designs and codes in this paper come from the following standard construction, described in [7, Proposition 1] and in [8]:

**Result 2.1.** Let $G$ be a finite primitive permutation group acting on the set $\Omega$ of size $n$. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $G_\alpha$ of $\alpha$. If

$$\mathcal{B} = \{\Delta^g : g \in G\}$$

and, given $\delta \in \Delta$,

$$\mathcal{E} = \{\{\alpha, \delta\}^g : g \in G\},$$

Then we have $\mathcal{B}$ and $\mathcal{E}$ as described in [8].
then $B$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with $n$ blocks, and $E$ forms the edge set of a regular connected graph of valency $|\Delta|$, with $G$ acting as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

3. The binary codes

In all the following we will take $G$ to be the simple alternating group $A_n$, where $n \geq 5$, in its natural primitive rank-3 action of degree $\binom{n}{2}$ on $\Omega^2$ where $\Omega = \{1, 2, \ldots, n\}$. For the orbits $\Delta$ of the stabilizer of a point, as described in Result 2.1, we take the one of length $2(n-2)$ and get a symmetric 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design $D$.

Alternatively let $n$ be any integer and let $T(n)$ denote the triangular graph with vertex set $P$ the $(\binom{n}{2})$ 2-subsets of a set $\Omega$ of size $n$. The 1-design $D = (P, B)$ will have point set $P$, and for each point (2-subset) $\{a, b\} \in P$, $a \neq b$, $a, b \in \Omega$, a block, which we denote by $\{a, b\}$, is defined in the following way:

$$\{a, b\} = \{\{a, x\}, \{b, y\} | x \neq a, b; y \neq a, b\}.$$  

Then,

$$B = \{\{a, b\} | a, b \in \Omega, a \neq b\}.$$  

The incidence vector of the block $\{a, b\}$ is then

$$v^{[a, b]} = \sum_{x \neq a} v^{\{a, x\}} + \sum_{y \neq b} v^{\{b, y\}}$$  

(1)

where, as usual with the notation from [1], the incidence vector of the subset $X \subseteq P$ is denoted by $v^X$. Since our points here are actually pairs of elements from $\Omega$, note that we are using the notation $v^{[a, b]}$ instead of $v^{\{a, b\}}$, as discussed in [1].

Further, if $a, b, c$ are distinct points in $\Omega$, we write

$$v^{[a, b, c]} = v^{[a, b]} + v^{[b, c]} + v^{[a, c]}$$  

(2)

to denote this vector of weight 3 in the ambient space. Notice also that for any distinct $a, b, c$,

$$v^{[a, b]} + v^{[a, c]} = v^{[b, c]}.$$  

(3)

To avoid trivial cases we will take $n \geq 5$. Then in all the following, $C^\perp$ will denote the dual code of the binary code of $D$ and of $T(n)$.

First we summarize some results on these codes, namely the number of words of minimum weight in $C^\perp$, and the automorphism group that we will be needing. The proofs can be found in [9].

**Result 3.1 ([9]).** For $n \geq 6$ and even, $C$ is an $[(\binom{n}{2}, n-2, 2(n-2)]_2$ code and $C^\perp$ is an $[(\binom{n}{2}, (\binom{n}{2}) - n-2, 3]_2$ code.
For $n \geq 5$ and odd, $C$ is an $\binom{n}{2}, n-1, n-1\} \subseteq 2$ code and $C'$ is an $\binom{n}{2}, \binom{n}{2} - n - 1, 3\} \subseteq 2$ code:

\[
\text{Aut}(C) = \begin{cases}
S_n & \text{if } n \neq 6, \\
PGL_4(2) \cong A_8 & \text{if } n = 6.
\end{cases}
\]

Moreover, the minimum weight of $C'$ for $n \geq 5$ is 3 and any word of the form $v_{[a, b, c]}$, where $a, b, c$ are distinct, is in $C'$. If $n \neq 6$, these are all the words of weight 3 in $C'$, and the number of words of weight 3 is thus $\binom{n}{3}$. If $n = 6$, further words of weight 3 have the form $v_{[a, b]} + v_{[c, d]} + v_{[e, f]}$ where $\Omega = \{a, b, c, d, e, f\}$; in this case there are 35 words of weight 3.

Now take $w$ to be a word of minimum weight in $C'$; in Section 4 below we determine the structures of $(A_n)_w$ and $(S_n)_w$, i.e., the stabilizers of $w$ in $A_n$ and in the automorphism group of the code respectively.

Since $A_n$ acts as an automorphism group of the code, Lemma 4.1 deals with the action of $A_n$ on the minimum-weight codewords of $C'$. Furthermore the automorphism group of $C'$ is the symmetric group $S_n$, so in Lemma 4.2 we consider the action of $S_n$.

4. Stabilizers of a minimum-weight codeword

In Lemmas 4.1 and 4.2 we deal with the stabilizers in $A_n$ and $S_n$ respectively of the minimum-weight codewords in $C'$ when $n \geq 5$. Notice that, unlike in Result 3.1 where a case study was carried out for when $n$ is even or $n$ is odd, in the lemmas given below no mention is made of the parity of $n$, since the results are valid for any $n$ provided that $n \geq 5$.

Lemma 4.1. Let $w$ be a word of minimum weight in $C'$. For $n \geq 7$, $(A_n)_w$ is a maximal subgroup of $A_n$ of index $\binom{n}{3}$. Furthermore $(A_n)_w \cong (A_{n-3} \times 3):2$. If $n = 5$ then $(A_5)_w \cong S_3$ and is maximal in $A_5$. Moreover, if $n = 6$, then $(A_6)_w \cong S_4$ or $(\mathbb{Z}_3 \times \mathbb{Z}_3):\mathbb{Z}_2$ where $(\mathbb{Z}_3 \times \mathbb{Z}_3):\mathbb{Z}_2$ is not a maximal subgroup of $A_6$.

Proof. Let $C_3 = \{w \in C' \mid wt(w) = 3\}$ (here $wt(w)$ represents the weight of a codeword $w$ in $C'$) denote the set of minimum-weight codewords in $C'$. Since $A_n$ is an automorphism group of $C'$ it preserves the weight class of $C'$; therefore it preserves $C_3$. Now since $A_n$ is $(n-2)$-transitive on $\Omega$ it is transitive on both pairs of letters of $\Omega$ and on triples of letters of $\Omega$, the latter of which are the $\binom{n}{3}$ points of $C_3$ according to Result 3.1.

Since $A_n$ acts transitively on $C_3$, it follows that $|C_3| = \frac{|A_n|}{|(A_n)_w|}$ and so $\binom{n}{3} = \frac{n!}{|\Omega|! |(A_n)_w|!}$ from which we deduce that $|(A_n)_w| = 3(n - 3)!$ and also that $|A_n:(A_n)_w| = \binom{n}{3}$. Now by a theorem of Liebeck et al. [10] we have that $(A_n)_w$ is a maximal subgroup of $A_n$. Using the Atlas [5] we deduce that a maximal subgroup of $A_n$ of index $\binom{n}{3}$ is isomorphic to the subgroup $(A_{n-3} \times 3):2$ whenever $n \geq 7$.

Now, let $C'_3$ be the set of minimum-weight codewords for $C'$ when $n = 5$. It follows from Result 3.1 that $|C'_3| = \binom{5}{3} = 10$. By taking $w \in C'_3$ and acting $A_5$ on $w$ we get that $w^{A_5} = C'_3$, from which we deduce that $A_5$ is transitive on $C'_3$. From the orbit stabilizer
the stabilizers

Lemma 4.3. \( (A_n)_w \approx S_3 \), and thus maximal in \( A_n \).

Finally if \( n = 6 \), let \( C_3 \) be the set of minimum-weight codewords in \( C^{-} \). Then by the

Result 3.1 we have that there are \( \binom{6}{3} \) = 20 words of minimum weight in \( C^{-} \) and an
additional 15 codewords of the form \( v^{[a,b]} + v^{[c,d]} + v^{[e,f]} \) and so \( |C_3| = 35 \). Now acting
\( A_6 \) on \( C_3 \) we get that \( C_3 \) splits into two orbits, namely \( C_{3a} \) and \( C_{3b} \), of lengths 15 and 20 respectively. Let \( w_a \in C_{3a} \) and \( w_b \in C_{3b} \). Then \( (A_6)_w \) is a subgroup of order 24 and thus maximal in \( A_6 \), and from the list of maximal subgroups of \( A_6 \) (see [5]) we deduce that

\( (A_6)_w \approx S_4 \).

Since \( |(A_6)_w| = 18 \), it is not a maximal subgroup of \( A_6 \). Using the Sylow subgroups of \( (A_6)_w \), we are able to determine that \( (A_6)_w \approx (\mathbb{Z}_3 \times \mathbb{Z}_3) : \mathbb{Z}_2 \). \( \square \)

Since \( \text{Aut}(C^{-}) = S_n \) for all \( n \geq 5 \), except when \( n = 6 \), in Lemma 4.2 we determine the stabilizers \( (S_n)_w \) by extending the results of \( A_n \) to \( S_n \). Note that if \( n = 6 \), we have that \( \text{Aut}(C^{-}) = A_8 \) (see Result 3.1). Thus for \( n = 6 \), we determine the structure of the stabilizer \( (A_8)_w \) of \( w \) in \( \text{Aut}(C^{-}) \).

Lemma 4.2. For \( n \geq 5 \), except when \( n = 6 \), \( (S_n)_w \) is a maximal subgroup of \( S_n \) of index \( \binom{n}{3} \). Moreover \( (S_n)_w \approx S_{n-3} \times S_3 \). If \( n = 6 \), then \( (A_8)_w \approx 2^{4}:(S_3 \times S_3) \).

Proof. As in the proof of Lemma 4.1, consider \( C_3 = \{ w \in C^{-} \mid \text{wt}(w) = 3 \} \), where \( n \geq 5 \) and \( n \neq 6 \), as the set of minimum weight codewords in \( C^{-} \). Since \( A_n \) acts transitively on \( C_3 \), so does \( \text{Aut}(C^{-}) = S_n \), and thus \( |C_3| = \frac{|S_n|}{|(S_n)_w|} \). Since \( |C_3| = \binom{n}{3} \), it follows that \( \binom{n}{3} = \frac{n!}{(n-3)!} \). Hence \( |(S_n)_w| = 6(n-3)! \). In addition we have that \( |S_n : (S_n)_w| = \frac{n!}{6(n-3)!} = \binom{n}{3} \). The maximality of \( (S_n)_w \) in \( S_n \) now follows since \( |(S_n)_w| = 6(n-3)! \). Thus \( (S_n)_w \approx S_{n-3} \times S_3 \), whenever \( n \geq 5 \) and \( n \neq 6 \).

Finally, for \( n = 6 \) we have that \( C^{-} \) is a \([15, 11, 3]_2 \) binary code whose automorphism group is the alternating group \( A_8 \approx PGL_4(2) \). Now let \( S \) be the set of minimum-weight codewords of \( C^{-} \) when \( n = 6 \). From Result 3.1 we have that \( S \) consists of \( \binom{6}{3} = 20 \), and an additional 15 codewords of the form \( v^{[a,b]} + v^{[c,d]} + v^{[e,f]} \), and \( A_8 \) preserves this set (see [9, Proposition 3.4]). Now, if we let \( w \in S \), and orbit \( S \) under \( A_8 \), we have that \( |S| = 35 = \frac{|S_3|}{|(A_8)_w|} \), and so \( |(A_8)_w| = \frac{|A_8|}{|S|} = \frac{20|160|}{35} = 576 \). Now from the Atlas (see Atlas [5]) we deduce that \( (A_8)_w \) is maximal in \( A_8 \) and also that \( (A_8)_w \approx 2^{4}:(S_3 \times S_3) \). \( \square \)

Lemma 4.3. \( (A_n)_w \) is a maximal normal subgroup of \( (S_n)_w \), for all \( n \geq 5 \), except when \( n = 6 \). If \( n = 6 \), \( (A_6)_w \) is neither maximal nor normal in \( (A_8)_w \).

Proof. It is obvious that \( (A_n)_w \leq (S_n)_w \). Since \( A_n \) is a maximal subgroup of \( S_n \), \( (A_n)_w \)
will also be a maximal subgroup of \( (S_n)_w \). The normality of \( (A_n)_w \) in \( (S_n)_w \) follows at once on finding the index of \( (A_n)_w \) in \( (S_n)_w \). Observe that \( |(S_n)_w : (A_n)_w| = \frac{6(n-3)!}{3(n-3)!} = 2 \), and so the result follows.

If \( n = 6 \), we have that \( |(A_8)_w : (A_6)_w| = 24 \) if \( w_a \in C_{3a} \) or \( |(A_8)_w : (A_6)_w| = 32 \) if \( w_b \in C_{3b} \). But \( (A_8)_w \approx 2^{4}:(S_3 \times S_3) \) has no maximal subgroup of index 24, and also it does not have a normal subgroup of such index. Similarly we can show that
\((A_8)_w \cong 2^4:(S_3 \times S_3)\) has neither a maximal subgroup of index 32 nor a normal subgroup of such index. □

Acknowledgements

The author acknowledges the hospitality of the Departamento de Matemática e Engenharia Geográfica at Universidade Agostinho Neto, Luanda, Angola, during the final preparation of this article.

References